(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年3 月28 日 (28.03.2002)

PCT

(10) 国際公開番号
WO 02/25457 A1

(51) 国際特許分類[7]: G06F 15/00

(21) 国際出願番号: PCT/JP00/06418

(22) 国際出願日: 2000 年9 月20 日 (20.09.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): シーエーアイ株式会社 (CAI CO., LTD.) [JP/JP]; 〒111-0042 東京都台東区寿2丁目10番10号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 龍 忠光 (RYU, Tadamitsu) [JP/JP]; 〒111-0031 東京都台東区千束3丁目5番5-201号 アジアハイツ Tokyo (JP).

(74) 代理人: 西森浩司(NISHIMORI, Koji); 〒107-0052 東京都港区赤坂4-3-1 共同ビル赤坂401号 葵特許事務所 Tokyo (JP).

(81) 指定国 (国内): CN, JP, KR, US.

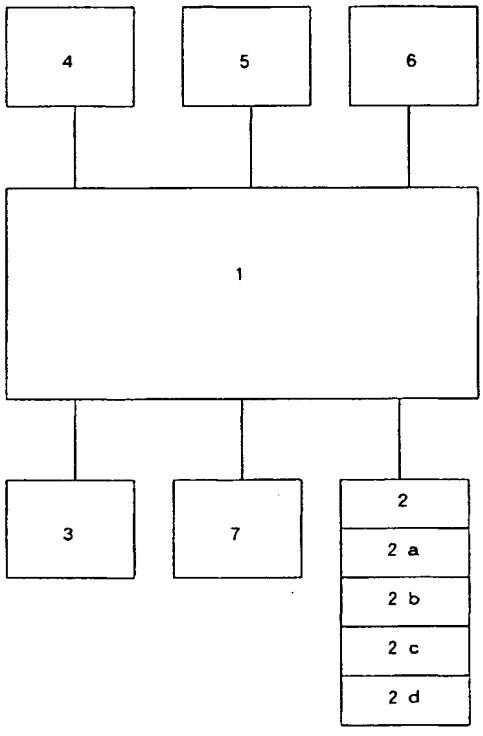
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: HYBRID PERSONAL AUTHENTICATING DEVICE, HYBRID PERSONAL AUTHENTICATING METHOD, AND RECORDED MEDIUM

(54) 発明の名称: ハイブリッド個人認証装置およびハイブリッド個人認証方法および記録媒体



(57) Abstract: A hybrid personal authenticating device for identifying and authenticating an individual, characterized by including any two to five authentication control means among face authentication control means (2a), pattern authentication control means/speech authentication control means (2b) personal information authentication control means (2c) means for controlling authentication by an IC card/magnetic card. By combining a plurality of authentication control means and controlling interaction as necessary, the authentication accuracy and authentication speed both being conventionally in an antinomy relation are both improved.

[続葉有]

WO 02/25457 A1

(57) 要約:

個人を識別し認証するためのハイブリッド個人認証装置であって、

イ）　顔認証制御手段（２ａ）

ロ）　紋認証制御手段・声話認証制御手段（２ｂ）

ハ）　個人情報認証制御手段（２ｃ）

ニ）　ＩＣカード・磁気カードによる認証制御手段

のいずれか二つないし五つの認証制御手段を含むことを特徴とする。

本発明は、複数の認証制御手段を組み合わせ、また、必要に応じて対話制御を行わせることにより、従来二律背反の関係にあった認証精度と認証速度の両方を向上させることができる。

明細書

ハイブリッド個人認証装置およびハイブリッド個人認証方法および記録媒体

技術の背景

本発明は、個人を識別し、認証するためのハイブリッド個人認証装置およびハイブリッド個人認証方法ならびにそれを記録した記録媒体に関する。特に、認識率が高く且つ認証速度が速いにもかかわらず高価なハードウエア・ソフトウエアを必要としない実用的なハイブリッド個人認証装置およびハイブリッド個人認証方法ならびにそれを記録した記録媒体に関する。

従来技術

個人を識別し、認証するための個人認証装置は、従来から公知である。例えば、以下のようなものがある。

1） 顔認証装置

人物の顔の特徴による認証を行う装置である（例．特開平１１－１６１７９１）。また、固有値による顔認識法は、「コンピュータによる顔の認識―サーベイ―」電子情報通信学会論文誌、Ｄ－ＩＩ、Ｖｏｌ．Ｊ８０－Ｄ－ＩＩ　Ｎｏ．８　ｐｐ２０３１－２０４６（１９９７年８月）に、Ｔｕｒｋらによる「Ｅｉｇｅｎｆａｃｅ（固有顔）法」として紹介されている。

2） 指紋認証装置

指紋の特徴による認証を行う装置である(例.特開平１１－９６３６３)。

3） こう彩認証装置

人物の目の特徴による認証を行う装置である（例．特開平１１－２１３１６４）。

4） 声紋認証装置

人物の発した声の特徴による認証を行う装置である（例．特開平１１－７３１９６）。

5） 声話認証装置

人物の話し方による特徴による認証を行う装置である（例．特開平１１－３５２９８４）。

6） ＩＣカード・磁気カード等による認証装置

ＩＣカードや磁気カード等を利用して認証を行う装置である。

しかし、実際問題として、上述した個人認証装置のうちＩＣカード等による認証装置以外の各々を単独で使用する場合には、認証精度を高めようとすれば、認証速度がきわめて遅くなるという問題があった。

また、上述した個人認証装置の各々を単独で使用すると認証精度は低くなるという問題があった。

また、認証中に、認証者が退屈してしまうという問題があった。

さらに、ＩＣカードや磁気カード等による認証装置を単独で使用する場合は、ＩＣカード等を必ず携帯していなければ認証できないという問題があった。

そこで、前記問題を解決するため、本発明は、複数の認証制御手段を組み合わせ、また、必要に応じて対話制御を行わせることにより、従来二律背反の関係にあった認証精度と認証速度の両方を向上させた実用性の高いハイブリッド個人認証装置およびハイブリッド個人認証方法を提供することを目的とする。

発明の開示

前記目的を達成するために、本発明は、第１に、個人を識別し認証するためのハイブリッド個人認証装置であって、下記イないしホのいずれか二つないし五つの認証制御手段を含むことを特徴とするハイブリッド個人認証装置を提供するものである。

イ） 顔認証制御手段

ロ） 声紋認証制御手段

ハ） 声話認証制御手段

ニ） 個人情報認証制御手段

ホ） ＩＣカード・磁気カードによる認証制御手段

すなわち、異なる種類の複数の認証制御手段を組み合わせることによって、一つの認証方法によっては速度を犠牲にするか、あるいは、高価なハードウエアを用いるかしなければ達成することができなかった認証精度を飛躍的に高めることができるところに特徴がある。また、認証速度を高めるために各認証方法の精度を低めたとしても、他の認証方法により認証精度を補完又は単一のものに比較して高めることができるので、単一の認証方法の場合に比較して認証速度を高めることもできるところに特徴がある。

また、第２に個人を識別し認証するためのハイブリッド個人認証装置であって、顔認証制御手段と、声紋または声話認証制御手段と、個人情報認証制御手

段と、を含むことを特徴とするハイブリッド個人認証装置を提供するものである。

すなわち、顔認証制御手段と声紋または声話認証制御手段と個人情報認証制御手段とを組み合わせることによって認証精度を高めようとするところに特徴がある。

また、第３に個人を識別し認証するためのハイブリッド個人認証装置であって、顔認証制御手段と、声紋または声話認証制御手段と、個人情報認証制御手段と、認証頻度管理制御手段と、を含むことを特徴とするハイブリッド個人認証装置を提供するものである。

すなわち、認証対象が膨大な場合、認証頻度管理制御手段により、全認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に各認証を行うことにより、認証速度を高めようとするところに特徴がある。

また、第４に個人を識別し認証するためのハイブリッド個人認証装置であって、顔認証制御手段と、声紋または声話認証制御手段と、個人情報認証制御手段と、認証頻度管理制御手段と、分類管理機能と、を含むことを特徴とするハイブリッド個人認証装置を提供するものである。

すなわち、認証対象が膨大な場合、分類管理機能により認証対象を分類し、そのうちの使用頻度の高い認証対象だけを認証頻度管理制御手段により抽出できるように認証対象を管理し、その管理された認証対象を基に各認証を行うことにより、さらに認証速度を高めようとするところに特徴がある。

また、第５に、第１ないし第４のいずれか一の場合のハイブリッド個人認証装置において、対話制御手段を設けたことを特徴とするハイブリッド個人認証装置を提供するものである。

すなわち、対話制御手段を待たせることにより、各認証方法への移行をスムーズなものにし、認証待ち時の体感認証速度を高めようとするところに特徴がある。

また、本発明は、第６に、個人を識別し認証するためのハイブリッド個人認証方法であって、下記イないしホのいずれか二ステップないし五ステップを含むことを特徴とするハイブリッド個人認証方法を提供するものである。

イ）　顔認証ステップ

ロ） 声紋認証ステップ

ハ） 声話認証ステップ

ニ） 個人情報認証ステップ

ホ）ＩＣカード・磁気カードによる認証制御手段

すなわち、異なる種類の複数の認証ステップを組み合わせることによって、一ステップの認証によっては速度を犠牲にするか、あるいは、高価なハードウエアを用いるかしなければ達成することができなかった認証精度を飛躍的に高めることができるところに特徴がある。また、認証速度を高めるために各認証ステップの精度を低めたとしても、他の認証ステップにより認証精度を補完又は単一のものに比較して高めることができるので、単一の認証方法の場合に比較して認証速度を高めることもできるところに特徴がある。

また、第７に、個人を識別し認証するためのハイブリッド個人認証方法であって、顔認証ステップと、声紋または声話認証ステップと、個人情報認証ステップと、を含むことを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、顔認証ステップと声紋または声話認証ステップと個人情報認証ステップとを組み合わせることによって認証精度を高めようとするところに特徴がある。

また、第８に、個人を識別し認証するためのハイブリッド個人認証方法であって、顔認証ステップと、声紋または声話認証ステップと、個人情報認証ステップと、認証頻度管理ステップと、を含むことを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、全認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に各認証を行うことにより、認証速度を高めようとするところに特徴がある。

また、第９に、個人を識別し認証するためのハイブリッド個人認証方法であって、顔認証ステップと、声紋または声話認証ステップと、個人情報認証ステップと、認証頻度管理ステップと、分類管理ステップとを含むことを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、分類管理ステップにより全認証対象を分類し適合する認証対象を抽出し、その中から使用頻度の高い認証対象だけを抽

出できるように認証対象を管理し、その管理された認証対象を基に各認証を行うことにより、認証速度を高めようとするところに特徴がある。

また、第１０に、個人を識別し認証するためのハイブリッド個人認証方法であって、個人情報認証ステップを実行し、声紋または声話認証ステップを実行し、顔認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、まず個人情報認証ステップにより認証対象を絞り込み、その後に声紋または声話認証ステップを実行することによりさらに認証対象を絞り込み、さらに顔認証ステップにより認証を行うことにより、認証精度を高めた上認証速度を高めようとするところに特徴がある。また、個人情報認証ステップを音声入力にて行えば、声紋または声話認証ステップも略同時に行うことができるのでさらに認証速度を高められるところに特徴がある。

また、第１１に、個人を識別し認証するためのハイブリッド個人認証方法であって、個人情報認証ステップを実行し、顔認証ステップを実行し、声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、まず個人情報認証ステップにより認証対象を絞り込み、その後に顔認証ステップにより認証を実行することによりさらに認証対象を絞り込み、さらに声紋または声話認証ステップを実行することにより、認証精度を高めた上認証速度を高めようとするところに特徴がある。また、個人情報認証ステップを音声入力にて行えば、声紋または声話認証ステップにも使用することができるのでさらに認証速度を高められるところに特徴がある。

また、第１２に、個人を識別し認証するためのハイブリッド個人認証方法であって、顔認証ステップを実行し、声紋または声話認証ステップを実行し、個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、まず近づいてきた認証者を顔認証ステップにより認証を実行することにより認証速度を高めた上、認証対象を絞り込み、さらに声紋または声話認証ステップを実行し、認証対象を絞り込み、さらに個人情報認証ステップにより認証対象を絞り込むことにより、認証精度を高めた上認証速度を高めようとするところに特徴がある。また、声紋または声話認証ステップには音声入力

を使うので、その入力を用いて個人情報認証ステップを行えば認証速度をさらに高められるところに特徴がある。

また、第１３に、個人を識別し認証するためのハイブリッド個人認証方法であって、顔認証ステップを実行し、個人情報認証ステップを実行し、声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、まず近づいてきた認証者を顔認証ステップにより認証を実行することにより認証速度を高めた上、認証対象を絞り込み、さらに個人情報認証ステップを実行し、認証対象を絞り込み、さらに声紋または声話認証ステップにより認証対象を絞り込むことにより、認証精度を高めた上認証速度を高めようとするところに特徴がある。また、個人情報認証ステップを音声入力にて行えば、声紋または声話認証ステップも略同時に行うことができるのでさらに認証速度を高められるところに特徴がある。

また、第１４に、個人を識別し認証するためのハイブリッド個人認証方法であって、声紋または声話認証ステップを実行し、顔認証ステップを実行し、個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、声紋または声話認証ステップにより認証対象を絞り込み、次に顔認証ステップを実行することにより認証対象を絞り込み、さらに個人情報認証ステップにより認証対象を絞り込むことにより、認証精度を高めた上認証速度を高めようとするところに特徴がある。また、声紋または声話認証ステップには音声入力を使うので、その入力を用いて個人情報認証ステップを行えば認証速度を高められるところに特徴がある。

また、第１５に、個人を識別し認証するためのハイブリッド個人認証方法であって、声紋または声話認証ステップを実行し、個人情報認証ステップを実行し、顔認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、声紋または声話認証ステップにより認証対象を絞り込み、次に個人情報認証ステップを実行することにより認証対象を絞り込み、さらに顔認証ステップにより認証対象を絞り込むことにより、認証精度を高めた上認証速度を高めようとするところに特徴がある。また、声紋または声話認証ステップに

は音声入力を使うので、その入力を用いて個人情報認証ステップを行えば認証速度を高められるところに特徴がある。

また、第１６に、個人を識別し認証するためのハイブリッド個人認証方法であって、認証頻度管理ステップを実行し、個人情報認証ステップを実行し、声紋または声話認証ステップを実行し、顔認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、全認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず個人情報認証ステップを実行し、次に個人情報認証ステップで絞り込まれた認証対象を基に声紋または声話認証ステップを実行し、さらに声紋または声話認証ステップにより絞り込まれた認証対象を基に顔認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第１７に、個人を識別し認証するためのハイブリッド個人認証方法であって、認証頻度管理ステップを実行し、個人情報認証ステップを実行し、顔認証ステップを実行し、声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、全認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず個人情報認証ステップを実行し、次に個人情報認証ステップで絞り込まれた認証対象を基に顔認証ステップを実行し、さらに顔認証ステップにより絞り込まれた認証対象を基に声紋または声話認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第１８に、個人を識別し認証するためのハイブリッド個人認証方法であって、認証頻度管理ステップを実行し、顔認証ステップを実行し、声紋または声話認証ステップを実行し、個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、全認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず顔認証ステップを実行し、次に顔認証ステップで絞り込まれた認証対象を基に声紋または声話認証ステップを実行し、さらに声紋または声話認証ステップにより絞り込まれた認証対象を基に個人情報認証ステップを実行することに

より、さらに認証速度を高めようとするところに特徴がある。

また、第１９に、個人を識別し認証するためのハイブリッド個人認証方法であって、認証頻度管理ステップを実行し、顔認証ステップを実行し、個人情報認証ステップを実行し、声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、全認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず顔認証ステップを実行し、次に顔認証ステップで絞り込まれた認証対象を基に個人情報認証ステップを実行し、さらに個人情報認証ステップにより絞り込まれた認証対象を基に声紋または声話認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第２０に、個人を識別し認証するためのハイブリッド個人認証方法であって、認証頻度管理ステップを実行し、声紋または声話認証ステップを実行し、顔認証ステップを実行し、個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、全認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず声紋または声話認証ステップを実行し、次に声紋または声話認証ステップで絞り込まれた認証対象を基に顔認証ステップを実行し、さらに顔認証ステップにより絞り込まれた認証対象を基に個人情報認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第２１に、個人を識別し認証するためのハイブリッド個人認証方法であって、認証頻度管理ステップを実行し、声紋または声話認証ステップを実行し、個人情報認証ステップを実行し、顔認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、全認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず声紋または声話認証ステップを実行し、次に声紋または声話認証ステップで絞り込まれた認証対象を基に個人情報認証ステップを実行し、さらに個人情報認証ステップにより絞り込まれた認証対象を基に顔認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第２２に、個人を識別し認証するためのハイブリッド個人認証方法であって、分類管理ステップを実行し、認証頻度管理ステップを実行し、個人情報認証ステップを実行し、声紋または声話認証ステップを実行し、顔認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、分類管理ステップを実行し、認証対象を絞り込み、その認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず個人情報認証ステップを実行し、次に個人情報認証ステップで絞り込まれた認証対象を基に声紋または声話認証ステップを実行し、さらに声紋または声話認証ステップにより絞り込まれた認証対象を基に顔認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第２３に、個人を識別し認証するためのハイブリッド個人認証方法であって、分類管理ステップを実行し、認証頻度管理ステップを実行し、個人情報認証ステップを実行し、顔認証ステップを実行し、声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、分類管理ステップを実行し、認証対象を絞り込み、その認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず個人情報認証ステップを実行し、次に個人情報認証ステップで絞り込まれた認証対象を基に顔認証ステップを実行し、さらに顔認証ステップにより絞り込まれた認証対象を基に声紋または声話認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第２４に、個人を識別し認証するためのハイブリッド個人認証方法であって、分類管理ステップを実行し、認証頻度管理ステップを実行し、顔認証ステップを実行し、声紋または声話認証ステップを実行し、個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、分類管理ステップを実行し、認証対象を絞り込み、その認証対象から使用頻度の高い認証対象だけを抽出できるように

認証対象を管理し、その管理された認証対象を基に、まず顔認証ステップを実行し、次に顔認証ステップで絞り込まれた認証対象を基に声紋または声話認証ステップを実行し、さらに声紋または声話認証ステップにより絞り込まれた認証対象を基に個人情報認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第２５に、個人を識別し認証するためのハイブリッド個人認証方法であって、分類管理ステップを実行し、認証頻度管理ステップを実行し、顔認証ステップを実行し、個人情報認証ステップを実行し、声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、分類管理ステップを実行し、認証対象を絞り込み、その認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず顔認証ステップを実行し、次に顔認証ステップで絞り込まれた認証対象を基に個人情報認証ステップを実行し、さらに個人情報認証ステップにより絞り込まれた認証対象を基に声紋または声話認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第２６に、個人を識別し認証するためのハイブリッド個人認証方法であって、分類管理ステップを実行し、認証頻度管理ステップを実行し、声紋または声話認証ステップを実行し、顔認証ステップを実行し、個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、分類管理ステップを実行し、認証対象を絞り込み、その認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず声紋または声話認証ステップを実行し、次に声紋または声話認証ステップで絞り込まれた認証対象を基に顔認証ステップを実行し、さらに顔認証ステップにより絞り込まれた認証対象を基に個人情報認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第２７に、個人を識別し認証するためのハイブリッド個人認証方法であって、分類管理ステップを実行し、認証頻度管理ステップを実行し、声紋ま

たは声話認証ステップを実行し、個人情報認証ステップを実行し、顔認証ステップを実行することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、認証対象が膨大な場合、分類管理ステップを実行し、認証対象を絞り込み、その認証対象から使用頻度の高い認証対象だけを抽出できるように認証対象を管理し、その管理された認証対象を基に、まず声紋または声話認証ステップを実行し、次に声紋または声話認証ステップで絞り込まれた認証対象を基に個人情報認証ステップを実行し、さらに個人情報認証ステップにより絞り込まれた認証対象を基に顔認証ステップを実行することにより、さらに認証速度を高めようとするところに特徴がある。

また、第２８に、全認証対象から認証頻度の高い認証対象を選択してａ認証対象とし、

下記ステップ１を実行し、

下記ステップ２を実行し、

下記ステップ３を実行することを特徴とするハイブリッド個人認証方法を提供するものである。

ステップ 1）下記イないしハのステップのいずれか一つを実行し、認証対象が見つからなかった場合は、全認証対象から個人情報認証ステップを実行して絞り込んだ認証対象をａ認証対象に追加して、前記追加数分をａ認証対象から削除して、再度

下記イないしハのステップのいずれか一つを実行する。

認証が確定した場合は、認証結果を出力する。

認証対象が複数ある場合はステップ２を実行する。

ステップ２）下記イないしハのステップであってステップ１で実行されていないいずれか一つを実行し、

認証対象が見つからなかった場合は、全認証対象から個人情報認証ステップを実行して絞り込んだ認証対象をａ認証対象に追加して、前記追加数分をａ認証対象から削除して、再度、ステップ１を実行する。

認証が確定した場合は、認証結果を出力する。

認証対象が複数ある場合はステップ３を実行する。

ステップ３）個人情報認証ステップを実行し、

認証対象が見つからなかった場合は、全認証対象から次に頻度の高い複数の認証対象を選択してａ認証対象とし、ステップ１を実行する。

認証が確定した場合は、認証結果を出力する。

認証対象が複数ある場合はステップ３を実行する。

イ）顔認証ステップ

ロ）個人情報認証ステップ

ハ）声紋または声話認証ステップ

すなわち、まず、全認証対象から頻度の高い認証対象をａ認証対象として抽出し、その後ステップ１において、認証を行い、認証対象が見つからない場合は全認証対象から個人情報認証にて認証対象となった認証対象をａ認証対象に追加することにより、再度全認証対象を認証対象にすることを避けることができるので、認証速度を高められるところに特徴がある。

また、ステップ１において認証対象が複数ある場合は、ステップ２においてステップ１と別の認証を行うことにより、認証精度を高められるところに特徴がある。また、認証対象が見つからない場合は全認証対象から個人情報認証にて認証対象となった認証対象をａ認証対象に追加することにより、再度全認証対象を認証対象にすることを避けることができるので、認証速度を高められるところに特徴がある。

また、ステップ２において認証対象が複数ある場合は、ステップ３において個人情報認証を行うことにより、認証精度を高められるところに特徴がある。また、ステップ３においてステップ１、２とは別の個人情報認証を繰り返すことにより、認証精度を高められるところに特徴がある。また、認証対象が見つからない場合は全認証対象から現在のａ認証対象とは別の頻度の高い認証対象を抽出してａ認証対象とすることにより、再度全認証対象を認証対象にすることを避けることができるので、認証速度を高められるところに特徴がある。

また、第２９に、分類管理ステップを実行した後に請求項２８に記載のハイブリッド個人認証方法を実施することを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、分類管理ステップを実行した後に第２８の場合に記載のハイブリッド個人認証方法を実施することにより、さらに認証対象を絞り込み認証速度をさらに高められるところに特徴がある。

また、第３０に、第６ないし第２９のいずれか一の場合に記載のハイブリッド個人認証方法に対話ステップを含むことを特徴とするハイブリッド個人認証方法を提供するものである。

すなわち、対話ステップを含むことにより、各認証ステップへの移行をスムーズなものにし、認証待ち時の体感認証速度を高めようとするところに特徴がある。

さらに、第３１に、第６ないし第３０のいずれか一の場合に記載のハイブリッド個人認証方法をコンピュータ装置に実行させるためのプログラムが記録されたコンピュータ読み取り可能な記録媒体を提供するものである。

すなわち、各認証ステップを実行させるためのプログラムをコンピュータに読取可能なように記録媒体に記録しておくことによりこの認証装置にこの認証方法を実行可能とすることができるところに特徴がある。

さらに、第３２に、請求項１ないし請求項５のいずれか一項に記載のハイブリッド個人認証装置において、前記顔認証制御手段は、固有値によって個人を識別し認証する機能であることを特徴とする。

顔認証制御手段が固有値によって個人を識別し認証するものであることにより、認証速度をさらに高められるところに特徴がある。

さらに、第３３に、請求項６ないし請求項３０のいずれか一項に記載のハイブリッド個人認証方法において、顔認証ステップは、固有値によって個人を識別し認証するステップであることを特徴とする。

顔認証ステップが固有値によって個人を識別し認証するものであることにより、認証速度をさらに高められるところに特徴がある。

ここで、顔認証制御手段またはステップとは、顔の特徴を例えばＣＣＤカメラ等のような画像入力手段により入力された情報を解析した顔の特徴と、データベース等の登録手段により登録されている顔の特徴とを比較し認証する機能またはステップである。

また、顔の固有値（固有顔）によって個人を識別し認証する機能またはステップとは、例えば、前述した論文「コンピュータによる顔の認識」で引用されたＴｕｒｋらによる「Ｅｉｇｅｎｆａｃｅ（固有顔）法」を用いて顔認識を行う機能またはステップを意味する。具体的には、多数の顔画像の濃淡値ベクトルの集合に対して主成分分析（ＰＣＡ）を適用し、固有顔と呼ばれる正規直交

基底を予め求めておき、これらの基底を用いて顔画像の濃淡値ベクトルのカーフネン・ローブ展開（Karhunen-Loeve 展開）を施すことによってパターンの次元圧縮された表現を求め、これを識別のための特徴ベクトルとするものである。

また、声紋認証制御手段またはステップとは、声紋を例えばマイク等のような音声入力手段により入力された情報を解析した声紋と、データベース等の登録手段により登録されている声紋とを比較し認証する機能またはステップである。

また、声話認証制御手段またはステップとは、例えばマイク等のような音声入力手段により入力された情報を解析した話者の話し方の特徴と、データベース等の登録手段により登録されている話者の話し方の特徴とを比較し認証する機能またはステップである。

また、個人情報認証制御手段またはステップとは、用意された質問事項に対して認証者の答えた内容と、データベース等の登録手段により登録されている認証者の内容とを比較し認証する機能またはステップである。

また、対話制御手段またはステップとは、音声入出力機能による対話により、認証や再認証を促す等、認証過程において次の操作を促すためにスピーカ等の音声出力機能を用いた音声出力やマイク等による音声入力機能による音声入力によりこのハイブリッド個人認証装置が認証者と対話をするための機能またはステップである。

また、認証頻度管理制御手段またはステップとは、認証対象を認証頻度で管理し、全認証対象のうち認証頻度の高い認証対象の何件かを抽出する機能またはステップである。すなわち、この機能またはステップは、認証確率の高い認証対象を絞り込んだ上で抽出することにより認証速度を高め、かつ適合性を高めるものである。

また、分類管理機能またはステップとは、認証対象をある分類、例えば、在籍部署や在籍している階数等に分類して管理しておき、認証を行う場所等によってその場所において最も認証頻度が高いであろう分類の認証対象を選択して抽出することにより認証対象を絞り込む機能またはステップである。

図面の簡単な説明

図１は、本発明の第１実施形態に係る装置概念図である。

図２は、本発明の第１実施形態に係る流れ図である。

図３は、本発明の第２実施形態に係る流れ図である。

図４は、本発明の第３実施形態に係る流れ図である。

図５は、本発明の第４実施形態に係る流れ図である。

図６は、本発明の第５実施形態に係る流れ図である

発明を実施する最良の形態

以下、図面に沿って、本発明に係るハイブリッド個人認証装置及びハイブリッド個人認証方法の実施形態を説明する。ただし、この実施形態の説明による例は、あくまでも実施の形態の一態様である。

以下、図１に基づき、本発明の第１実施形態に係る装置の概念について説明する。

この実施形態にかかるハイブリッド個人認証装置は、制御手段１と、記憶手段２と、結果出力手段３と、音声入力手段４と、音声出力手段５と、画像入力手段６と、一時記憶手段７とを含んで構成される。

前記制御手段１は、ＣＰＵ等の演算や他の手段を制御する等の処理を行う。他の各手段はこの制御手段１に接続され制御される。

また、前記記憶手段２には、顔認証機能を果たすべく顔認証ステップと、声紋認証機能・声話認証機能を果たすべく声紋・声話認証ステップと、個人情報認証機能を果たすべく個人情報認証ステップとをコンピュータ装置に実行させるためのプログラム２ａ、２ｂ、２ｃ及びデータベース２ｄとが記録されている。そして、記憶手段２は前記制御手段１に接続され、データベース２ｄのデータに基づき各認証ステップが制御･実行される。このデータベース２ｄには、顔認証情報、声紋・声話認証情報、個人情報のための認証情報が一対になって登録されている。前記記憶手段２には、例えばハードディスク等の磁気記録媒体のほか、ＤＶＤ等のような光学的記録媒体も含まれる。

また、前記結果出力手段３とは、ＣＲＴ等のように視覚等により認証結果を参照できる等の認証結果を表示する、あるいは、オートロック等やＡＴＭ等の認証結果を用いて起動する等の認証結果を出力する手段をいう。これもまた、前記制御手段１に接続され、必要なときに認証結果を出力する。

前記音声入力手段４とは、マイクロフォン等のように音声を入力できる手段である。また、前記音声出力手段５とは、スピーカ等のように音声を出力でき

る手段である。また、前記画像入力手段６とは、ＣＣＤカメラ等のように画像を入力できる手段である。これらもまた、前記制御手段１に接続され、必要なときに入力し、出力される。

前記一時記憶手段７とは、メモリ等のように、データ等を一時的に記憶しておく手段である。これも前記制御手段１に接続され、制御される。

前述のように本実施形態にかかるハイブリッド個人認証装置は構成されているので、画像入力手段６から入力した顔の特徴とデータベース２ｄの顔の特徴データとを比較して顔認証ステップを行い、認証結果を一時記憶手段７に保存しておく。そのステップの終了後、その一時記憶手段７に保存されている認証結果をもとに、音声入力手段４の声紋とデータベース２ｄに登録されている声紋データとを比較し、声紋認証ステップを実行する。そして、同様に認証結果を一時記憶手段７に保存しておく。

さらに、それらステップの終了後、その一時記憶手段７に保存されている認証結果をもとに、個人情報認証ステップを実行する。この個人情報認証ステップは、まず音声出力手段５により必要な情報を認証者に問いかけ、認証者が音声入力手段４により、その質問事項に解答する。そして、その解答とデータベース２ｄ中に登録されているデータとを比較することにより認証を行うのである。

本実施形態に係るハイブリッド個人認証装置は前述のように構成されているので、認証速度を優先させるために個々の個人認証方法の精度を落としても、別の個人認証方法により認証精度を補完又は高めることができるので、全体としての認証速度が増加し、精度の高い個人認証を行うことができるのである。

以下、図２の第１実施形態に係る流れ図に基づき、本実施形態に係るハイブリッド個人認証装置の実施の流れを説明する。

第１に、顔認証ステップを実行する(ステップ１)。まず、ハイブリッド個人認証装置は、「カメラの前に顔を向けてください。」等の音声を音声出力手段５から出力し、認証者に画像入力手段６の前に顔を向けるように促す。次に、本装置の画像入力手段６は、認証者の顔の画像を本装置に入力する。次に、本装置は、この顔の画像の特徴を抽出し、この顔の特徴とデータベース２ｄに登録されている顔の特徴とを比較する(ステップ２)。個人の顔の認識を、個人々々が有する顔の特徴、すなわち、固有値によって識別するように構成することが

できる。固有値（固有顔）を用いた手法は、例えば、前述した論文「コンピュータによる顔の認識」で引用されたＴｕｒｋらによる「Ｅｉｇｅｎｆａｃｅ（固有顔）法」がある。これらの顔認識を行うことにより、識別率９５％の精度で認識速度を飛躍的に向上させることができる。

このときうまく画像が入力できなくて認証結果が０件であるような場合には、再度「カメラの前に顔を向けてください。」等の音声を音声出力手段５から出力し再認証を促す。そして、認証がうまくできた場合は、本装置は、一時記憶手段７に認証結果を保存しておき音声出力手段５または結果出力手段３から「認証結果は５０件でした。」等の結果を出力し、認証者に認証結果を知らせる(ステップ３)。

第２に声紋・声話認証ステップを実行する(ステップ４)。まず、本装置は、「マイクに何か話し掛けてください。」等の音声を音声出力手段５から出力し、認証者に音声入力手段４に話し掛けるように促す。次に、本装置の音声入力手段４は、認証者の音声を本装置に入力する。次に、本装置は、この声紋を抽出し、その情報と前記の一時記憶手段７に保存されている認証結果に基づきデータベース２ｄに登録されている声紋とを比較する(ステップ５)。このときうまく音声が入力できなくて認証結果が０件であるような場合には、再度「マイクに何か話し掛けてください。」等の音声を音声出力手段５から出力し再認証を促す。そして、認証がうまくできた場合は、本装置は、一時記憶手段７に認証結果を保存しておき音声出力手段５または結果出力手段３から「認証結果は８件でした。」等の結果を出力し、認証者に認証結果を知らせる(ステップ６)。

第３に個人情報認証ステップを実行する(ステップ７)。まず、本装置は、「あなたの生年月日はいつですか。」等の音声を音声出力手段５から出力し、認証者に音声入力手段４に話し掛けるように促す。次に、本装置の音声入力手段４は、認証者の解答を本装置に入力する。次に、本装置は、その解答と前記の一時記憶手段７に保存されている認証結果に基づきデータベース２ｄに登録されている個人情報とを比較する(ステップ８)。このとき、うまく音声が入力できなくて認証結果が０件であるような場合には、再度「マイクに何か話し掛けてください。」等の音声を音声出力手段５から出力し再認証を促す。そして、認証がうまくできた場合は、本装置は、最終結果を出力する(ステップ９)。

前記では、説明の便宜上、顔認証、声紋（または声話）認証、個人情報認証

の順に実施する場合を説明したが、本発明はこの順に限らず、顔認証、声紋（または声話）認証、個人情報認証を使ったさまざまな組み合わせの順において適応できるものである。

前述のようなハイブリッド個人認証装置およびハイブリッド個人認証方法を使用することにより、前記出力装置としていろいろなものを使い、前記出力された最終結果を利用すれば、例えば、家の鍵として、銀行等のＡＴＭ等のキャッシュカードとして、電子商取引の鍵として、等さまざまな分野への実用的な応用が考えられる。

以下、図３に基づき、本発明に係る第２実施形態を説明する。

なお、装置については、第１実施形態と同様のものである。

まず、このハイブリッド個人認証装置は、音声出力手段５により例えば「名前を教えてください。」等の個人情報認証情報の解答を促すような質問を問いかける(ステップ１０)。それにより認証者は、個人情報認証情報である解答を行う(ステップ１１)。図３の場合は「龍崎忠輝です。」と名前を答えている。このときの解答は、音声入力手段４から入力される。

そして、その音声入力された解答とデータベース２ｄ中に登録されている。個人情報認証情報との照合を行い、認証対象を絞り込む(ステップ１２)。これにより、個人情報認証ステップが実行される。

次にその絞り込まれた認証対象をもとに、前記で音声入力された声紋とデータベース２ｄ中に登録されている。声紋認証情報との照合を行う(ステップ１３)。これにより、声紋認証ステップが実行される。

次に、このハイブリッド個人認証装置は、音声出力手段５により、「顔をカメラに向けてください。」と認証者に顔をカメラの方向に向けるように促し、画像入力手段６により顔の特徴を入力する(ステップ１４)。

そして、前記で絞り込まれた認証対象をもとにその入力された顔の特徴とデータベース２ｄ中に登録されている顔認証情報との照合を行う(ステップ１５)。これにより、顔認証ステップを実行する。ところで、前記声紋認証で認証が確定した場合でも再確認としてこのステップを実行するのが望ましい。

前記では、説明の便宜上、個人情報認証、声紋（または声話）認証、顔認証の順に実施する場合を説明したが、本発明はこの順に限らず、顔認証、声紋（または声話）認証、個人情報認証を使ったさまざまな組み合わせの順において適

応できるものである。

前記のように実施し、その認証結果を用いて、結果出力手段３に出力することにより(ステップ１６)、さまざまな「鍵」として使用することが可能となるのである。

さらに、本実施形態によれば、個人情報認証により絞り込まれた認証対象のみが次のステップの認証対象となるので、認証速度が速く認証精度が高いより実用性のある認証が可能となるのである。

以下、図４に基づき、本発明に係る第３実施形態を説明する。

なお、装置については、第１実施形態と同様のものである。

本実施形態は、認証対象データの件数が例えば１０万件等の莫大な件数である場合、頻繁に用いられる頻度の高い認証対象データを、例えば１００件だけ抽出し書き換え可能なメモリ、すなわち、一時記憶手段７に記録しておく。そして、その認証対象データを対象に認証を行うことにより、認証速度を高め、かつ適合性をも高めようとするものである。つまり、抽出された認証頻度の高い認証対象データの件数は、全件数よりもはるかに少ないので、認証速度が高く、また、その抽出されたデータの認証確率は高いという特性を利用したものである。

ところで、図４中および以下の(ａ)行程とは認証頻度管理ステップであり、(ｂ)行程とは個人情報認証後認証対象抽出ステップであり、(ｃ)行程とは声紋認証後認証対象抽出ステップである。

第１に、認証頻度管理ステップを実行する(ステップ２０)。まず、このハイブリッド個人認証装置を起動すると、記憶手段２中にあるデータベース２ｄが起動する。ここで、データベース２ｄには仮に１０万件の認証対象データが存在すると仮定する。このハイブリッド個人認証装置の制御手段１は、その１０万件の認証対象データの中から、その使用前に頻繁に用いられていたとする認証対象データを例えば１００件を選択して抽出する＜(ａ) 工程＞。

ここで、前記で認証対象データを例えば１００件選択することとしたが、この数は、記憶手段２または一時記憶手段７の容量や制御手段１の速度等により適宜選択できるものである。また、それら認証対象データの選択方法は、例えば、データベース２ｄ中の認証対象データ中に「使用頻度」なるフィールドを設けておき、前記「使用頻度」がカウントされるように管理しておく。そして、

このハイブリッド個人認証装置で認証される度にその数が増加するようにしておく。さらに、このハイブリッド個人認証装置の制御手段１はこの「使用頻度」の数の大きい順に並べ替え、その上位１００件を選択して抽出すればよい。

第２に、個人情報認証ステップを実行する(ステップ２１)。このステップでは、第２実施形態と同様に、このハイブリッド個人認証装置が音声出力手段５により例えば「名前を教えてください。」等の個人情報認証情報の解答を促すような質問を問いかけ、それにより認証者は、個人情報認証情報である解答を行う。このときの解答は、音声入力手段４から入力される。そして、その音声入力された解答と（ａ）行程（認証頻度管理ステップ）により抽出された認証対象データとの照合を行い、認証対象がある場合は、（ｂ）行程（個人情報認証後認証対象抽出ステップ）を実行する(ステップ２２)。（ｂ）行程とはすなわち、（ａ）行程により抽出された認証対象データのうち、個人情報認証ステップにより認証対象となった認証対象データのみを絞り込んで抽出する行程である。

また、個人情報認証ステップで認証対象が見つからなかった場合は、（ａ）行程で抽出された認証対象データを消去し、データベース２ｄ中から次に頻度の高い別の上位１００件の認証対象データを新たに抽出し、その認証対象データを基に前記と同様に個人情報認証ステップを実行する。この処理は、認証対象が発見されるまで繰り返す。

第３に、声紋認証ステップを実行する(ステップ２３)。すなわち、（ｂ）行程（個人情報認証後認証対象抽出ステップ）で抽出され絞り込まれている認証対象データを基に声紋認証を行う。このステップでは、個人情報認証により絞り込まれた認証対象データの声紋と音声入力手段４により入力された声紋とを比較して認証を行う。そして、（ｃ）行程（声紋認証後認証対象抽出ステップ）を実行する(ステップ２４)。（ｃ）行程とはすなわち、（ｂ）行程で抽出された認証対象データのうち声紋認証を行った結果である認証対象データのみに絞り込んで抽出する行程である。

このとき、認証対象データが１件の場合、すなわち認証が確定した場合は、認証結果を結果出力手段３に出力して終了する(ステップ２６)。ここで、この声紋認証において認証を行うための声紋は、前記で行った個人情報認証において音声入力手段４により音声入力された解答の音声を解析した声紋を用いると効率的である。

第４に、顔認証ステップを実行する(ステップ２５)。すなわち、(ｃ)行程(声紋認証後認証対象抽出ステップ)で抽出され絞り込まれた認証対象データを基に顔認証を行う。顔認証は、第２実施形態と同様に、ＣＣＤカメラ等の画像入力手段６により顔の特徴を画像にて入力し、この顔の特徴と声紋認証により絞り込まれた認証対象データの顔の特徴とを比較することにより認証を行う。そして、認証結果を結果出力手段３に出力して終了する(ステップ２６)。

このとき、認証結果が確定しなかったとき、すなわち、認証対象データが１件ではなかったときは、この顔認証により絞り込まれた認証対象データを基に、再度、別の個人情報認証、例えば、住所等を入力させる等を行うことにより認証結果を確定し、認証結果を結果出力手段３に出力する。

前記の再度行う別の個人情報認証の方法とは、例えば前記の個人情報認証と同様にこのハイブリッド個人認証装置が音声出力手段５により「住所を教えてください。」と認証者に住所等を解答するように促す。認証者はそれに対し「台東区～です。」と答えることにより、その解答を音声入力手段４により入力する。この入力された個人情報認証情報と前記顔認証により絞り込まれた認証対象データの個人情報認証情報とを比較することにより認証を行う。

前記では、説明の便宜上、個人情報認証、声紋（または声話）認証、顔認証の順に実施する場合を説明したが、本発明はこの順に限らず、顔認証、声紋（または声話）認証、個人情報認証を使ったさまざまな組み合わせの順において適応できるものである。

前記のように第３実施形態によれば、使用頻度の高い認証対象を抽出して管理することにより、認証対象を絞り込んで認証処理を行えるので、認証速度をさらに高めることができる。また、各認証ステップにより順次認証対象を絞り込んで行くので、追加して認証速度を高めることが出来るのである。さらに、使用頻度の高い認証対象を抽出してそれを対象に認証しているので、認証確率を高くすることができる。

以下、図５に基づき、本発明に係る第４実施形態を説明する。

なお、装置については、第１実施形態と同様のものである。

本実施形態は、認証対象データの件数が例えば１０万件等の莫大な件数である場合、予め分類されている認証対象データのうち適合性の高いと判断される分類の認証対象データを抽出しておき、その分類の認証対象データのうち頻繁

に用いられる頻度の高い認証対象データを、例えば１００件だけ抽出しておき、その認証対象データを対象に認証を行うことにより、認証速度を高め、かつ適合性をも高めようとするものである。つまり、適合性の高い分類の認証対象を選択することにより適合性を高めた上でその中でも認証頻度の高い認証対象データを抽出することにより、認証精度が高くかつ認証対象が少ないので認証速度が高いという特性を利用したものである。

ところで、図５中および以下の（ａ）行程とは分類管理ステップであり、（ｂ）行程とは認証頻度管理ステップであり、（ｃ）行程とは個人情報認証ステップであり、（ｄ）行程とは個人情報認証後認証対象抽出ステップであり、（ｅ）行程とは顔認証ステップであり、（ｆ）行程とは顔認証後認証対象抽出ステップであり、（ｇ）行程とは声紋（または声話）認証ステップである。

第１に（ａ）行程（分類管理ステップ）を実行する(ステップ３０)。すなわち、認証対象を複数に分類しておき、その分類によりその認証場所において適合性の高い認証対象データを抽出し絞り込むステップを実行する。ここで、分類とは、例えば所属する部署や建物の階数等任意の属性による分類である。例えば、認証する場所（このハイブリッド個人認証装置が置かれている場所）が２階の場合は、この在籍する階数が「２階」の分類の認証対象データを抽出しておけば適合性が高くなり、認証対象が絞り込まれるので認証速度が高くなる。この性質を利用したのがこのステップである。

前記ステップを実施するためには、例えば、認証対象データに「分類」なるフィールドを設けておき、分類毎にデータが入力または指定できるようにしておき、その「分類」フィールドを検索できるようにしておく。そして、認証対象場所において適合性の高い分類の認証対象データを検索して抽出すればよい。

第２に、（ａ）行程で抽出した認証対象データを対象に、（ｂ）行程（認証頻度管理ステップ）を実行する(ステップ３１)。まず、このハイブリッド個人認証装置を起動すると、記憶手段２中にあるデータベース２ｄが起動する。ここで、データベース２ｄには仮に１０万件の認証対象データが存在すると仮定する。そして、前記（ａ）行程にて２万件が抽出されたとする。このハイブリッド個人認証装置の制御手段１は、その２万件の認証対象データの中から、その使用前に頻繁に用いられていたとする認証対象データを例えば１００件を選択して抽出する。

ここで、前記で認証対象データを例えば１００件選択することとしたが、この数は、記憶手段２または一時記憶手段７の容量や制御手段１の速度等により適宜選択できるものである。また、それら認証対象データの選択方法は、例えば、データベース２ｄ中の認証対象データ中に「使用頻度」なるフィールドを設けておき、前記「使用頻度」がカウントされるように管理しておく。そして、このハイブリッド個人認証装置で認証される度にその数が増加するようにしておく。さらに、このハイブリッド個人認証装置の制御手段１はこの「使用頻度」の数の大きい順に並べ替え、その上位１００件を選択して抽出すればよい。

第３に、（ｃ）行程（個人情報認証ステップ）を実行する(ステップ３２)。このステップでは、第２・第３実施形態と同様に、このハイブリッド個人認証装置が音声出力手段５により例えば「名前を教えてください。」等の個人情報認証情報の解答を促すような質問を問いかけ、それにより認証者は、個人情報認証情報である解答を行う。このときの解答は、音声入力手段４から入力される。そして、その音声入力された解答と（ｂ）行程（認証頻度管理ステップ）により抽出された認証対象データとの照合を行い、認証対象がある場合は、（ｄ）行程（個人情報認証後認証対象抽出ステップ）を実行する(ステップ３３)。（ｄ）行程とはすなわち、（ｂ）行程により抽出された認証対象データのうち、（ｃ）行程（個人情報認証ステップ）により認証対象となった認証対象データのみを絞り込んで抽出する行程である。

また、（ｃ）行程（個人情報認証ステップ）で認証対象が見つからなかった場合は、（ｂ）行程で抽出された認証対象データを消去し、（ａ）行程で抽出された認証対象データ中から次に頻度の高い別の上位１００件の認証対象データを新たに抽出し置き換える(ステップ３９)。その認証対象データを基に前記と同様に個人情報認証ステップを実行する。この処理は、認証対象が発見されるまで繰り返す。

この繰り返しによっても認証対象が発見されない場合は、図示されていないが、分類による認証対象データの選択を廃止して、データベース２ｄ中の全認証対象データにおいて頻度の高い上位１００件の認証対象データを抽出して、その認証対象データを基に前記と同様に個人情報認証ステップを実行する。これでも認証対象が発見されない場合は、全認証対象データ中から次に頻度の高い別の上位１００件の認証対象データを新たに抽出し、その認証対象データを

基に前記と同様に個人情報認証ステップを実行する。この処理は、認証対象が発見されるまで繰り返す。

第４に、（ｅ）行程（顔認証ステップ）を実行する(ステップ３４)。すなわち、（ｄ）行程（個人情報認証後認証対象抽出ステップ）で抽出され絞り込まれている認証対象データを基に顔認証を行う。顔認証は、第２・第３実施形態と同様に、ＣＣＤカメラ等の画像入力手段６により顔の特徴を画像にて入力し、この顔の特徴と個人情報認証により絞り込まれた認証対象データの顔の特徴とを比較することにより認証を行う。そして、（ｆ）行程（顔認証後認証対象抽出ステップ）を実行する(ステップ３５)。（ｆ）行程とはすなわち、（ｄ）行程で抽出された認証対象データのうち顔認証を行った結果である認証対象データのみに絞り込んで抽出する行程である。

このとき、認証対象データが１件の場合、すなわち認証が確定した場合は、認証結果を結果出力手段３に出力して終了する(ステップ３７)。

第５に、（ｇ）行程（声紋（または声話）認証ステップ）を実行する(ステップ３６)。すなわち、（ｆ）行程（顔認証後認証対象抽出ステップ）で抽出され絞り込まれた認証対象データを基に声紋（または声話）認証を行う。声紋認証は、（ｆ)行程で抽出され絞り込まれた認証対象データ中の声紋の特徴と音声入力手段４により入力された音声の声紋の特徴とを比較することにより行う。ここで、この声紋認証において認証を行うための声紋は、前記で行った個人情報認証において音声入力手段４により音声入力された解答の音声を解析した声紋を用いると効率的である。

最後に、その認証結果を結果出力手段３に出力して終了する(ステップ３７)。

このとき、認証結果が確定しなかったとき、すなわち、認証対象データが１件ではなかったときは、この声紋認証により絞り込まれた認証対象データを基に、再度、別の個人情報認証、例えば、住所等を入力させる等を行う(ステップ３８)ことにより認証結果を確定し、認証結果を結果出力手段３に出力する。

前記の再度行う別の個人情報認証の方法とは、例えば前記の個人情報認証と同様にこのハイブリッド個人認証装置が音声出力手段５により「住所を教えてください。」と認証者に住所等を解答するように促し、認証者はそれに対し「台東区～です。」と答えることにより、その解答を音声入力手段４により入力し、この入力された個人情報認証情報と前記声紋・声話認証により絞り込まれた認

証対象データの個人情報認証情報とを比較することにより認証を行うのである。

前記では、説明の便宜上、個人情報認証、顔認証、声紋（または声話）認証の順に実施する場合を説明したが、本発明はこの順に限らず、顔認証、声紋（または声話）認証、個人情報認証を使ったさまざまな組み合わせの順において適応できるものである。

前記のように第４実施形態によれば、適合性の高い分類の認証対象を選択した上で使用頻度の高い認証対象を抽出して管理することにより、認証対象を絞り込んで認証処理を行えるので、第３実施形態の場合に追加して認証速度をさらに高めることができる。また、適合性の高い分類の認証対象を選択した上で使用頻度の高い認証対象を抽出して管理しているので、適合性及び認証確率を高めた上で認証精度を高くすることができる。

以下、図６に基づき、本発明に係る第５実施形態を説明する。

なお、装置については、第１実施形態と同様のものである。

本実施形態は、ある認証ステップを実行した結果、認証対象が見つからなかった場合に、個人情報認証によって認証対象を絞り込んで認証対象件数を少なくすることにより処理時間を減少させ、認証が確定した場合は直ちに認証結果を出力することにより認証速度を高め、認証が確定しなかった場合、すなわち、認証対象件数が１件以上の場合は別の認証ステップを実行することにより認証精度を高めるものである。

このハイブリッド個人認証装置によって認証が開始されたと判断された場合、例えば、認証開始ボタンが押下された場合や、このハイブリッド個人認証装置において画像入力手段６に認証対象者が入力された場合にループを抜ける処理を組み込んでおいた場合において、認証者が近づいて来て画像入力手段６に認証者の画像入力があった場合、まず、分類管理ステップ１０１を実施する。

すなわち、第４実施形態で説明した（ａ）行程（分類管理ステップ）と同様なステップを実施する。ここで、この分類管理ステップ１０１を実施するか否かは、本発明においては任意である。すなわち、この分類管理ステップ１０１を実施しない場合も本発明に該当する。しかし、この分類管理ステップ１０１を実施すれば、適合性が増加し、実施しない場合よりも認証確率及び認証速度を高めることが可能となる。

次に、認証頻度管理ステップ１０２を実施する。すなわち、第３実施形態で

説明した認証頻度管理ステップ、第４実施形態で説明した（ｂ）行程（認証頻度管理ステップ）と同様なステップを実施する。

次に、ａ認証ステップ１０３を実施する。ａ認証とは、顔認証、声紋または声話認証、個人情報認証のうちのいずれか一つの認証である。以下、ａ認証が例えば顔認証である場合を例に説明する。このステップは分類管理ステップ１０１及び認証頻度管理ステップ１０２（分類管理ステップ１０１が実施されない場合は認証頻度管理ステップ１０２）において抽出された認証対象を基に顔認証を行う。顔認証は、認証対象データの顔の特徴と、画像入力手段６により入力された顔の特徴とを比較して行う。前述のように固有値を用いて個人々々を識別認証すると、認証速度を早くすることができる。

顔認証の画像入力手段６による顔の特徴の入力は、例えば、このハイブリッド個人認証装置において画像入力手段６に認証者が入力された場合にループを抜ける処理を組み込んでおき、このハイブリッド個人認証装置に認証者が近づいてきた時に画像入力手段６により顔の特徴が入力されるとすれば、認証速度をさらに高めることができる。

次に、ａ認証対象件数による判断ステップ１０４を実施する。前記ａ認証ステップ１０３の結果により分岐するステップであり、前記の例では顔認証による結果により下記ａ）からｃ）の３つの場合に分岐する。ここで、ａ認証（前記例では顔認証）により認証対象となった件数（ａ認証対象件数）をｘとする。

ａ）ｘ＝０の場合、すなわち認証対象が発見されなかった場合

まず、全認証対象または前記分類管理ステップ１０１において抽出された認証対象を基に個人情報認証ステップ１１０を実施する。

次に、前記個人情報認証ステップ１１０により認証対象となった認証対象を前記認証頻度管理ステップ１０２の実施により絞り込まれた認証対象（以下、「Ａ認証対象」とする。）に追加し、追加した認証対象データの件数分の低頻度認証対象データをＡ認証対象から除外する（認証頻度管理ステップ１０２の一態様）。

次に、再度Ａ認証対象を基にａ認証ステップ１０３を実施する。

ここで、個人情報認証ステップ１１０は、第２から第４実施形態と同様に、例えば、このハイブリッド個人認証装置が音声出力手段５により「名前を教えてください。」と出力することにより問いかけ、それに認証者が「私は龍崎忠輝

です。」と解答することにより、その解答を音声入力手段４により入力し、その入力された解答の個人情報認証情報（この例では名前）と全認証対象データまたは分類管理ステップ１０２により分類され抽出された認証対象データにある個人情報認証情報（この例では名前）を比較して認証を行う。これを行うには、このハイブリッド個人認証装置に実施された場合のカウンタ（実施される毎にカウントされる）を設けておき、このステップが実施された場合に制御手段１がこのカウンタを参照して、そのカウンタの示す数値によりそれぞれ別の個人情報認証、例えば、住所・電話番号・役職等による個人情報認証ステップ１１０を実施できるようにしておけばよい。

ｂ）ｘ＝１の場合、すなわち、認証が確定した場合

認証結果出力ステップ１０９を実施する。すなわち、認証結果を結果出力手段３に出力して終了する。

ｃ）ｘ≧１の場合、すなわち、認証が確定せず認証対象が複数ある場合

まず、ａ認証ステップ１０３により絞られた認証対象を基にｂ認証ステップ１０５を実施する。

次にｂ認証対象件数による判断ステップ１０６を実施する。

ここで、ｂ認証とは、顔認証、声紋または声話認証、個人情報認証のうちのいずれか一つの認証であり且つａ認証で行われなかった種類の認証である。上記例ではａ認証が顔認証なので、以下ｂ認証が例えば声紋（または声話）認証である場合を例に説明する。このステップはａ認証（前記例では顔認証）ステップ１０３において抽出された認証対象を基に声紋(または声話)認証を行う。声紋（または声話）認証は、予め記録されていた認証対象データの声紋の特徴と、音声入力手段４により入力された声紋の特徴とを比較して行う。この声紋（または声話）認証の入力は例えば、このハイブリッド個人認証装置が音声出力手段５により何か問いかけ、それに対して認証者が何か答えることによりその解答の音声を音声入力手段４から入力するとよい。

また、ｂ認証対象件数による判断ステップ１０６は、前記ｂ認証ステップ１０５の結果により分岐するステップであり、前記の例では声紋（または声話）認証による結果により下記ｄ）からｆ）の３つの場合に分岐する。ここで、ｂ認証（前記例では声紋（または声話）認証）により認証対象となった件数（ｂ認証対象件数）をｙとする。

ｄ）ｙ＝０の場合、すなわち認証対象が発見されなかった場合

まず、全認証対象または前記分類管理ステップ１０１において抽出された認証対象を基に個人情報認証ステップ１１０を実施する。

次に、前記個人情報認証ステップ１１０により認証対象となった認証対象を前記認証頻度管理ステップ１０２の実施により絞り込まれた認証対象（以下、「Ａ認証対象」とする。）に追加し、追加した認証対象データの件数分の低頻度認証対象データをＡ認証対象から除外する（認証頻度管理ステップ１０２の一態様）。

次に、再度Ａ認証対象を基にａ認証ステップ１０３を実施する。

ここで、個人情報認証ステップ１１０は、前記で説明した個人情報認証ステップ１１０そのものである。前記同様に音声の入出力による対話を行うことにより行えばよい。また前記と同様にこれを実施するには、このハイブリッド個人認証装置には実施された場合のカウンタ（実施される毎にカウントされる）を設けておき、一度このステップが実施された場合は制御手段１がそのカウンタを参照して、そのカウンタの示す数値によりそれぞれ別の個人情報認証、例えば、住所・電話番号・役職等による個人情報認証ステップ１１０を実施できるようにしておけばよい。

ｂ）ｙ＝１の場合、すなわち、認証が確定した場合

認証結果出力ステップ１０９を実施する。すなわち、認証結果を結果出力手段３に出力して終了する。

ｃ）ｙ≧１の場合、すなわち、認証が確定せず認証対象が複数ある場合

まず、ｂ認証ステップ１０５により絞られた認証対象を基に個人情報認証ステップ１０７を実施する。

次に個人情報認証対象件数による判断ステップ１０８を実施する。

ここで、個人情報認証ステップ１０７とは、前記個人情報認証ステップ１１０と基本的には同様のステップである。ただし、認証を行う認証対象は、前記ｂ認証ステップ１０５により絞り込まれた認証対象である。

また、個人情報認証対象件数による判断ステップ１０８とは前記個人情報認証ステップ１０７の結果により分岐するステップであり、その認証による結果により下記ｇ）からｉ）の３つの場合に分岐する。ここで、個人情報認証により認証対象となった件数（個人情報認証対象件数）をｚとする。

ｇ）ｚ＝０の場合、すなわち認証対象が発見されなかった場合

まず、認証頻度管理１０２を実施する。ここで、前記の認証頻度管理１０２の実施により抽出され選択されている認証対象（一番認証頻度の高い複数（例えば１００件）の認証対象）とは別の次に高認証頻度の複数（例えば１００件）の認証対象を抽出し、それをＡ認証対象とする。全ての認証方法において認証されなかったのであるからＡ認証対象を新たなものにすることにより認証確率を高めるためである。

次に、再度Ａ認証対象を基にａ認証ステップ１０３を実施する。

ｈ）ｚ＝１の場合、すなわち、認証が確定した場合

認証結果出力ステップ１０９を実施する。すなわち、認証結果を結果出力手段３に出力して終了する。

ｉ）ｚ≧１の場合、すなわち、認証が確定せず認証対象が複数ある場合まず、個人情報認証ステップ１０７により絞られた認証対象を基に再度個人情報認証ステップ１０７を実施する。ただし、再度行う個人情報認証ステップ１０７は、個人情報認証情報を変更したもので行う。個人情報認証情報の変更は、例えば１回目が「住所」であった場合は、２回目は「電話番号」、３回目は「役職」等このステップを実施する毎に行う。この変更を行うには、このハイブリッド個人認証装置には実施された場合のカウンタ（実施される毎にカウントされる）を設けておき、一度このステップが実施された場合は制御手段１がそのカウンタを参照して、そのカウンタの示す数値によりそれぞれ別の個人情報認証、例えば、住所・電話番号・役職等による個人情報認証ステップ１１０を実施できるようにしておけばよい。

次に個人情報認証対象件数による判断ステップ１０８を実施する。

前記のように本実施形態によれば、適合性の高い認証対象を順次抽出することにより、認証速度が高まり、かつ、認証確率を高めることができる。また、認証により認証対象が発見されなかった場合には別の認証確率の高い認証対象を抽出して認証を行うので、全認証対象を認証対象として認証を行う場合に比し認証速度を高めることができる。また、各認証を行ったときにその認証が確定した時点ですぐに認証を終了するので、認証速度が高い。さらに、認証対象が複数発見された場合は、さらに別の認証を行うので認証確率を高くすることができる。

本発明に係るハイブリッド個人認証装置およびハイブリッド個人認証方法を用いて認証できなかったときには、対話によって再度認証を促し、再認証を行うことにより、認証精度を高めることが可能となる。

また、各認証制御手段および各認証ステップを組み合わせたことにより、個々の認証方法のみで認証できなかったものも認証することが可能となる。

また、個々の認証速度を速くすると認証精度が低くなるが、各認証制御手段および各認証ステップを組み合わせたことにより、個々の認証精度を下げても認証精度が高まるので、認証速度が速くかつ認証精度の高い個人認証が可能となるので、実用性が高いハイブリッド個人認証装置およびハイブリッド個人認証方法を提供することが可能となる。

また、対話を交わしながら認証を行うので、体感認証速度が高まるので、認証者が退屈せずに認証を行うことが可能となる。

また、個人情報認証により認証対象を絞り込んだ後に各認証ステップを実行することができるので、認証速度が増加し、認証精度の高いより実用性のあるハイブリッド個人認証装置およびハイブリッド個人認証方法を提供することが可能となる。

また、一時的に使用頻度の高い認証対象を絞り込んで抽出しておき、その絞り込まれた認証対象を基に個人情報認証、声紋・声話認証、顔認証と順次絞り込んで行くことにより、認証速度がさらに増加し、より実用性のあるハイブリッド個人認証装置およびハイブリッド個人認証方法を提供することが可能となる。

また、このハイブリッド個人認証装置を使用する目的・場所等により認証対象を分類させておけるので、使用する目的・場所等により選択する認証対象の分類を指定しておけば、認証確率、認証速度ともに高めることが可能となる。

さらに、使用頻度の高い認証対象を絞り込んで抽出しておき認証を行った場合において、一認証ステップで認証対象が発見されなかったときは、全認証対象を基に個人情報認証を行って、前記で絞り込まれた頻度の高い認証対象に追加することにより認証速度、認証確率を高めることができる。また、次回の認証からこの追加された認証対象を基に認証を行えば、経験則としての認証確率を高めることができる。

請求の範囲

1． 個人を識別し認証するためのハイブリッド個人認証装置であって、下記イないしホのいずれか二つないし五つの認証制御手段を含むことを特徴とするハイブリッド個人認証装置。

イ） 顔認証制御手段

ロ） 声紋認証制御手段

ハ） 声話認証制御手段

ニ） 個人情報認証制御手段

ホ） ＩＣカード・磁気カードによる認証制御手段

2． 個人を識別し認証するためのハイブリッド個人認証装置であって、

顔認証制御手段と、

声紋または声話認証制御手段と、

個人情報認証制御手段と、

を含むことを特徴とするハイブリッド個人認証装置。

3． 個人を識別し認証するためのハイブリッド個人認証装置であって、

顔認証制御手段と、

声紋または声話認証制御手段と、

個人情報認証制御手段と、

認証頻度管理制御手段と、

を含むことを特徴とするハイブリッド個人認証装置。

4． 個人を識別し認証するためのハイブリッド個人認証装置であって、

顔認証制御手段と、

声紋または声話認証制御手段と、

個人情報認証制御手段と、

認証頻度管理制御手段と、

分類管理機能と、

を含むことを特徴とするハイブリッド個人認証装置。

5． 請求項１ないし請求項４のいずれかに記載のハイブリッド個人認証装置において、対話制御手段が設けられていることを特徴とするハイブリッド個人認証装置。

6． 個人を識別し認証するためのハイブリッド個人認証方法であって、下記

イないしホのいずれか二ステップないし五ステップを含むことを特徴とするハイブリッド個人認証方法。

イ） 顔認証ステップ

ロ） 声紋認証ステップ

ハ） 声話認証ステップ

ニ） 個人情報認証ステップ

ホ） ＩＣカード・磁気カードによる認証ステップ

７． 個人を識別し認証するためのハイブリッド個人認証方法であって、

顔認証ステップと、

声紋または声話認証ステップと、

個人情報認証ステップと、

を含むことを特徴とするハイブリッド個人認証方法。

８． 個人を識別し認証するためのハイブリッド個人認証方法であって、

顔認証ステップと、

声紋または声話認証ステップと、

個人情報認証ステップと、

認証頻度管理ステップと、

を含むことを特徴とするハイブリッド個人認証方法。

９． 個人を識別し認証するためのハイブリッド個人認証方法であって、

顔認証ステップと、

声紋または声話認証ステップと、

個人情報認証ステップと、

認証頻度管理ステップと、

分類管理ステップと、

を含むことを特徴とするハイブリッド個人認証方法。

１０． 個人を識別し認証するためのハイブリッド個人認証方法であって、

個人情報認証ステップを実行し、

声紋または声話認証ステップを実行し、

顔認証ステップを実行することを特徴とするハイブリッド個人認証方法。

１１． 個人を識別し認証するためのハイブリッド個人認証方法であって、

個人情報認証ステップを実行し、

顔認証ステップを実行し、

声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法。

１２．　個人を識別し認証するためのハイブリッド個人認証方法であって、

顔認証ステップを実行し、

声紋または声話認証ステップを実行し、

個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法。

１３．　個人を識別し認証するためのハイブリッド個人認証方法であって、

顔認証ステップを実行し、

個人情報認証ステップを実行し、

声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法。

１４．　個人を識別し認証するためのハイブリッド個人認証方法であって、

声紋または声話認証ステップを実行し、

顔認証ステップを実行し、

個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法。

１５．　個人を識別し認証するためのハイブリッド個人認証方法であって、

声紋または声話認証ステップを実行し、

個人情報認証ステップを実行し、

顔認証ステップを実行することを特徴とするハイブリッド個人認証方法。

１６．　個人を識別し認証するためのハイブリッド個人認証方法であって、

認証頻度管理ステップを実行し、

個人情報認証ステップを実行し、

声紋または声話認証ステップを実行し、

顔認証ステップを実行することを特徴とするハイブリッド個人認証方法。

１７．　個人を識別し認証するためのハイブリッド個人認証方法であって、

認証頻度管理ステップを実行し、

個人情報認証ステップを実行し、

顔認証ステップを実行し、

声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法。

１８．　個人を識別し認証するためのハイブリッド個人認証方法であって、

認証頻度管理ステップを実行し、

顔認証ステップを実行し、

声紋または声話認証ステップを実行し、

個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法。

１９．　個人を識別し認証するためのハイブリッド個人認証方法であって、

認証頻度管理ステップを実行し、

顔認証ステップを実行し、

個人情報認証ステップを実行し、

声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法。

２０．　個人を識別し認証するためのハイブリッド個人認証方法であって、

認証頻度管理ステップを実行し、

声紋または声話認証ステップを実行し、

顔認証ステップを実行し、

個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法。

２１．　個人を識別し認証するためのハイブリッド個人認証方法であって、

認証頻度管理ステップを実行し、

声紋または声話認証ステップを実行し、

個人情報認証ステップを実行し、

顔認証ステップを実行することを特徴とするハイブリッド個人認証方法。

２２．　個人を識別し認証するためのハイブリッド個人認証方法であって、

分類管理ステップを実行し、

認証頻度管理ステップを実行し、

個人情報認証ステップを実行し、

声紋または声話認証ステップを実行し、

顔認証ステップを実行することを特徴とするハイブリッド個人認証方法。

２３．　個人を識別し認証するためのハイブリッド個人認証方法であって、

分類管理ステップを実行し、

認証頻度管理ステップを実行し、

個人情報認証ステップを実行し、

顔認証ステップを実行し、

声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法。

２４．　個人を識別し認証するためのハイブリッド個人認証方法であって、

分類管理ステップを実行し、

認証頻度管理ステップを実行し、

顔認証ステップを実行し、

声紋または声話認証ステップを実行し、

個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法。

２５．　個人を識別し認証するためのハイブリッド個人認証方法であって、

分類管理ステップを実行し、

認証頻度管理ステップを実行し、

顔認証ステップを実行し、

個人情報認証ステップを実行し、

声紋または声話認証ステップを実行することを特徴とするハイブリッド個人認証方法。

２６．　個人を識別し認証するためのハイブリッド個人認証方法であって、

分類管理ステップを実行し、

認証頻度管理ステップを実行し、

声紋または声話認証ステップを実行し、

顔認証ステップを実行し、

個人情報認証ステップを実行することを特徴とするハイブリッド個人認証方法。

２７．　個人を識別し認証するためのハイブリッド個人認証方法であって、

分類管理ステップを実行し、

認証頻度管理ステップを実行し、

声紋または声話認証ステップを実行し、

個人情報認証ステップを実行し、

顔認証ステップを実行することを特徴とするハイブリッド個人認証方法。

２８．　全認証対象から認証頻度の高い認証対象を選択してａ認証対象とし、

下記ステップ１を実行し、

下記ステップ２を実行し、

下記ステップ３を実行することを特徴とするハイブリッド個人認証方法。

ステップ1）下記イないしハのステップであっていずれか一つを実行し、

認証対象が見つからなかった場合は、全認証対象から個人情報認証ステップを実行して絞り込んだ認証対象をａ認証対象に追加して、前記追加数分をａ認証対象から削除して、再度

下記イないしハのステップであっていずれか一つを実行する。

認証が確定した場合は、認証結果を出力する。

認証対象が複数ある場合はステップ２を実行する。

ステップ２）下記イないしハのステップであってステップ１で実行されていないいずれか一つを実行し、

認証対象が見つからなかった場合は、全認証対象から個人情報認証ステップを実行して絞り込んだ認証対象をａ認証対象に追加して、前記追加数分をａ認証対象から削除して、再度

ステップ１を実行する。

認証が確定した場合は、認証結果を出力する。

認証対象が複数ある場合はステップ３を実行する。

ステップ３）個人情報認証ステップを実行し、

認証対象が見つからなかった場合は、全認証対象から次に頻度の高い複数の認証対象を選択してａ認証対象とし、ステップ１を実行する。

認証が確定した場合は、認証結果を出力する。

認証対象が複数ある場合はステップ３を実行する。

イ）顔認証ステップ

ロ）個人情報認証ステップ

ハ）声紋または声話認証ステップ

２９．　分類管理ステップを実行した後に請求項２８に記載のハイブリッド個

人認証方法を実施することを特徴とするハイブリッド個人認証方法。

３０．　請求項６ないし請求項２９のいずれか一項に記載のハイブリッド個人認証方法に対話ステップを含むことを特徴とするハイブリッド個人認証方法。

３１．　請求項６ないし請求項３０のいずれか一項に記載のハイブリッド個人認証方法をコンピュータ装置に実行させるためのプログラムが記録されたコンピュータ読み取り可能な記録媒体。

３２．　請求項１ないし請求項５のいずれか一項に記載のハイブリッド個人認証装置において、前記顔認証制御手段は、固有値によって個人を識別し認証する機能であることを特徴とするハイブリッド個人認証装置。

３３．　請求項６ないし請求項３０のいずれか一項に記載のハイブリッド個人認証方法において、顔認証ステップは、固有値によって個人を識別し認証するステップであることを特徴とするハイブリッド個人認証方法。

図 1

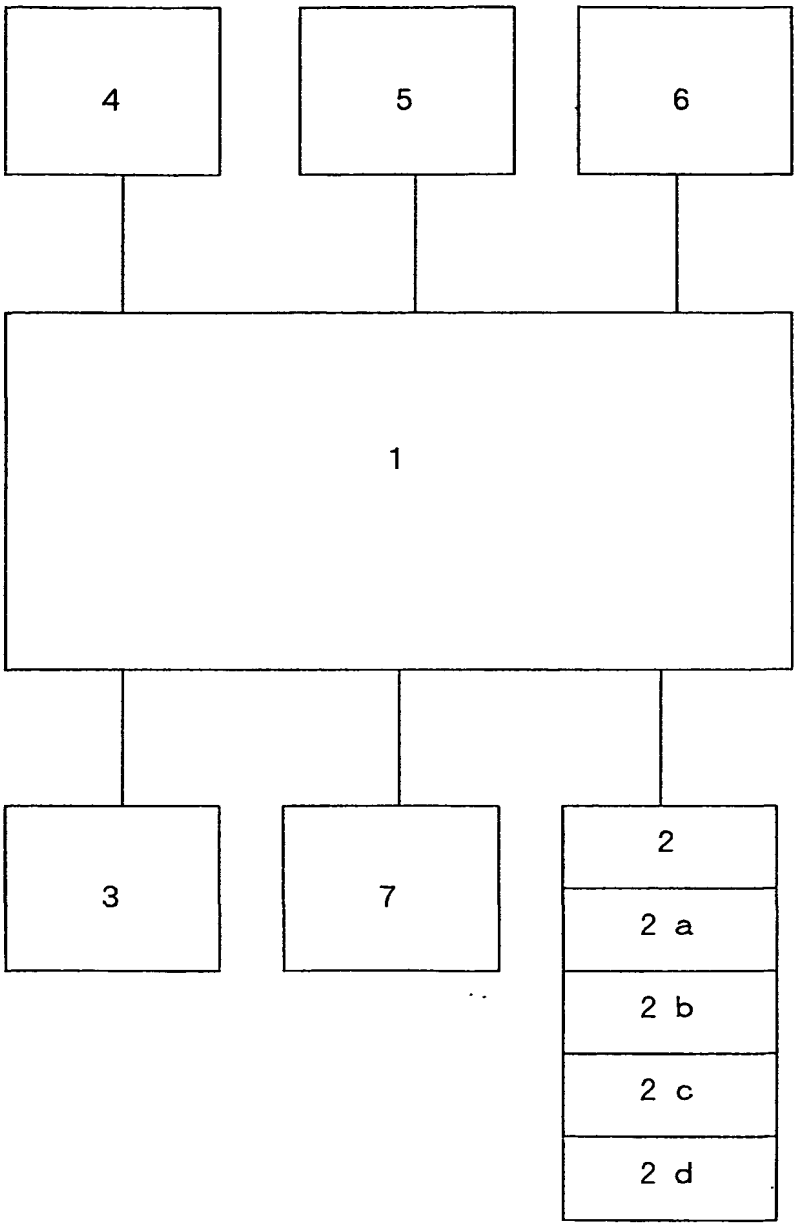


図 2

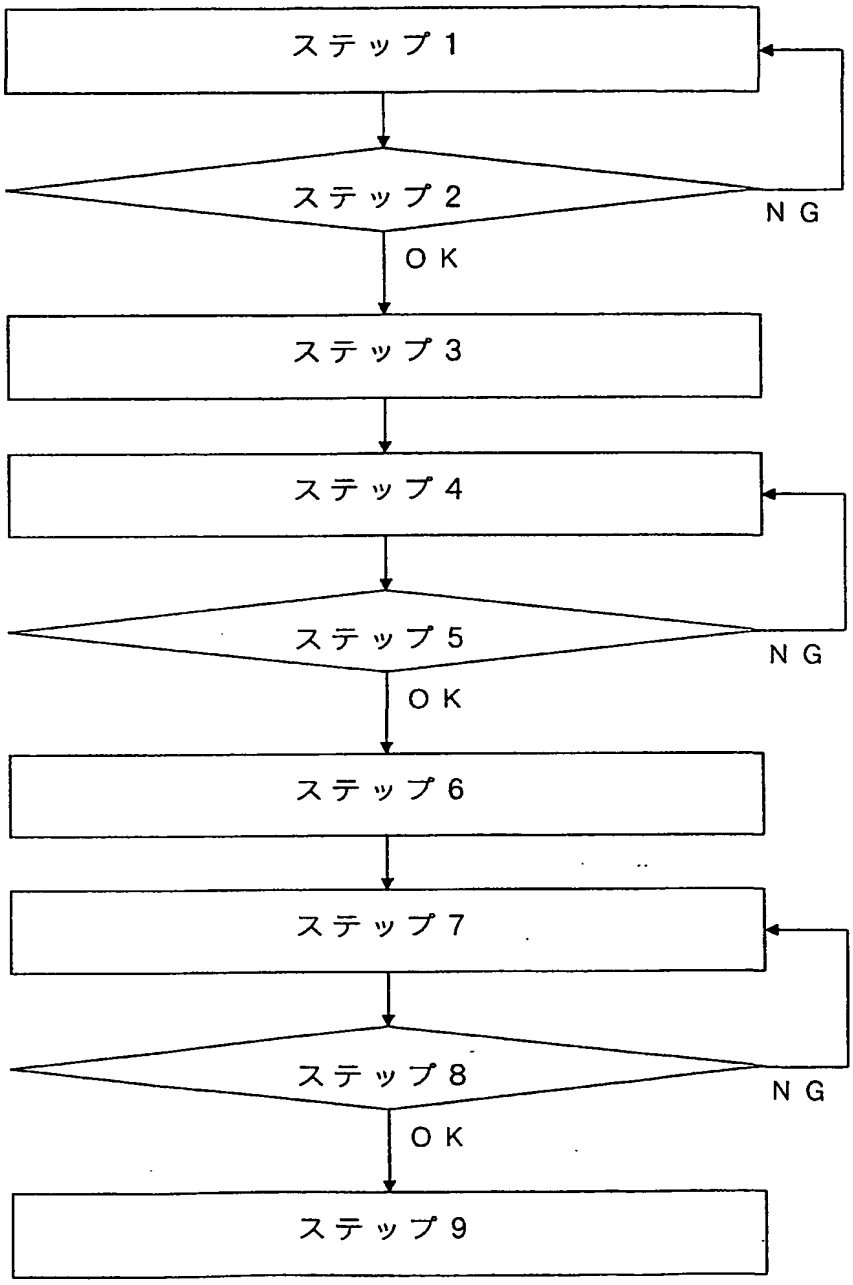

ステップ 1
ステップ 2
N G
O K
ステップ 3
ステップ 4
ステップ 5
N G
O K
ステップ 6
ステップ 7
ステップ 8
N G
O K
ステップ 9

図 3

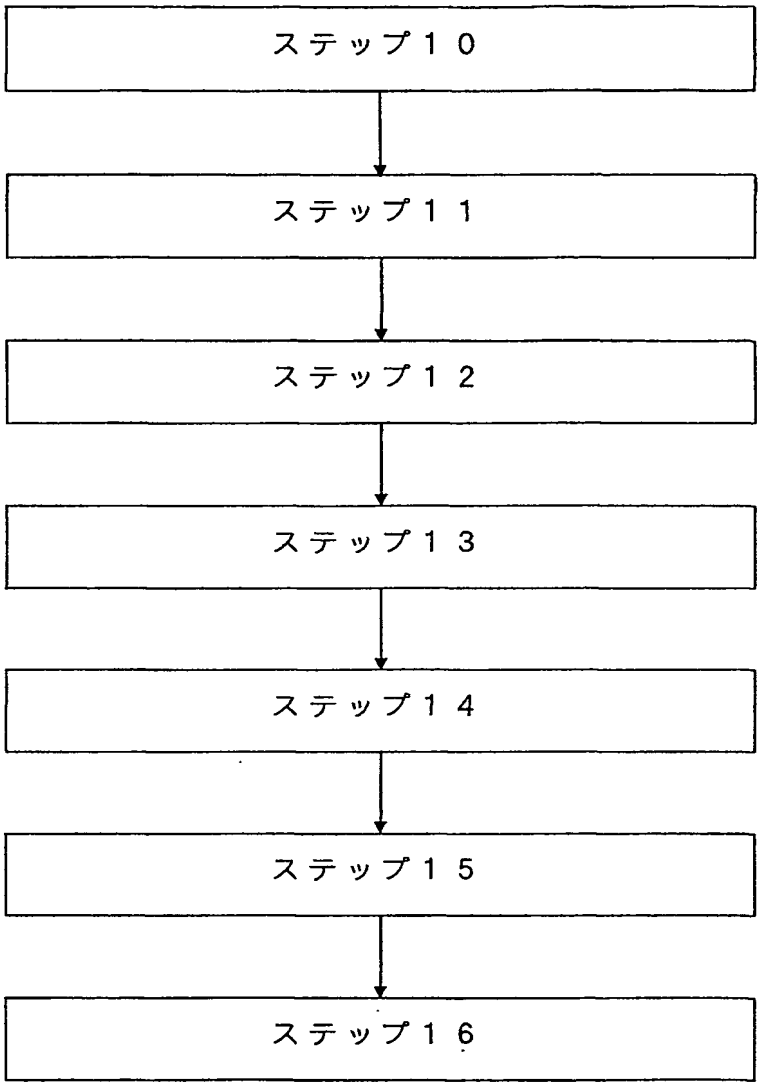


図４

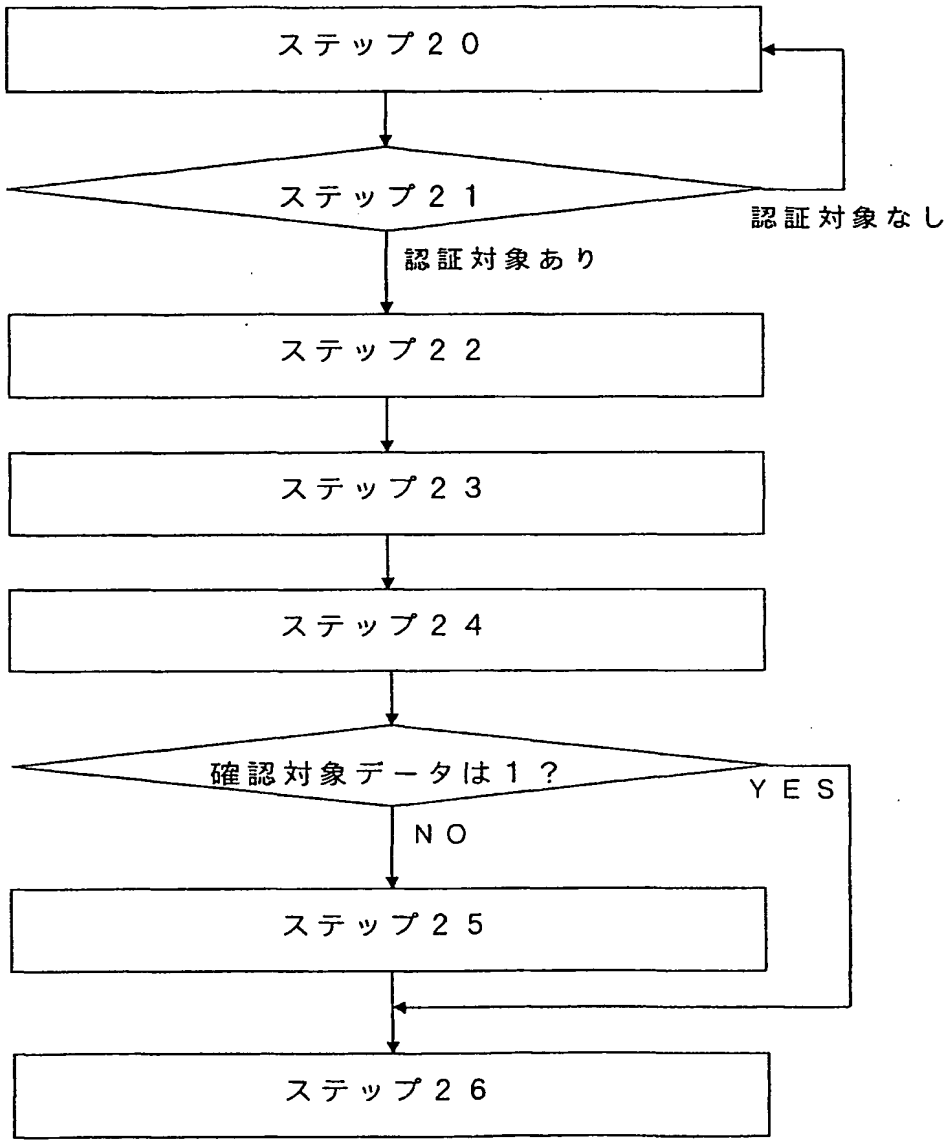

ステップ２０
ステップ２１
認証対象なし
認証対象あり
ステップ２２
ステップ２３
ステップ２４
確認対象データは１？
ＹＥＳ
ＮＯ
ステップ２５
ステップ２６

図 5

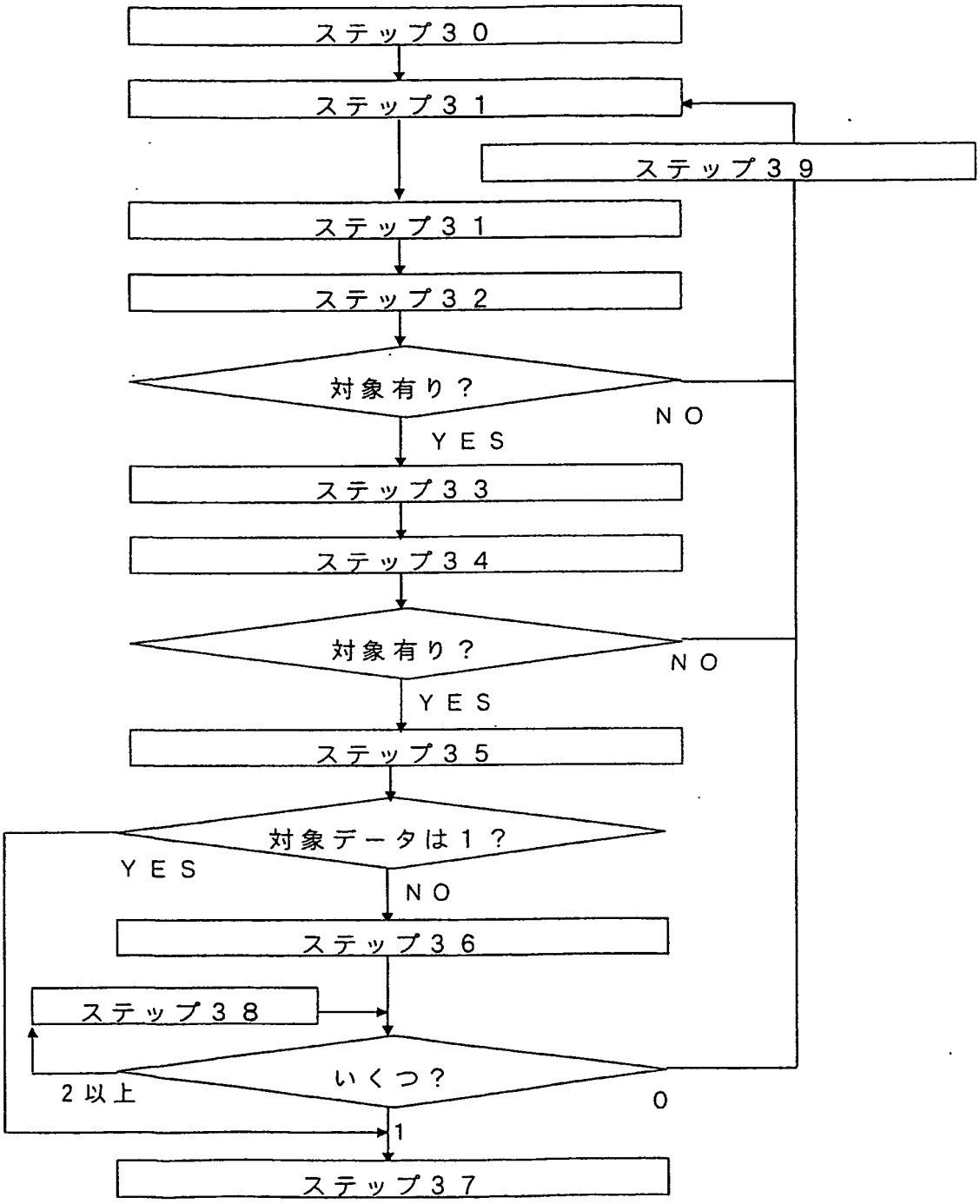
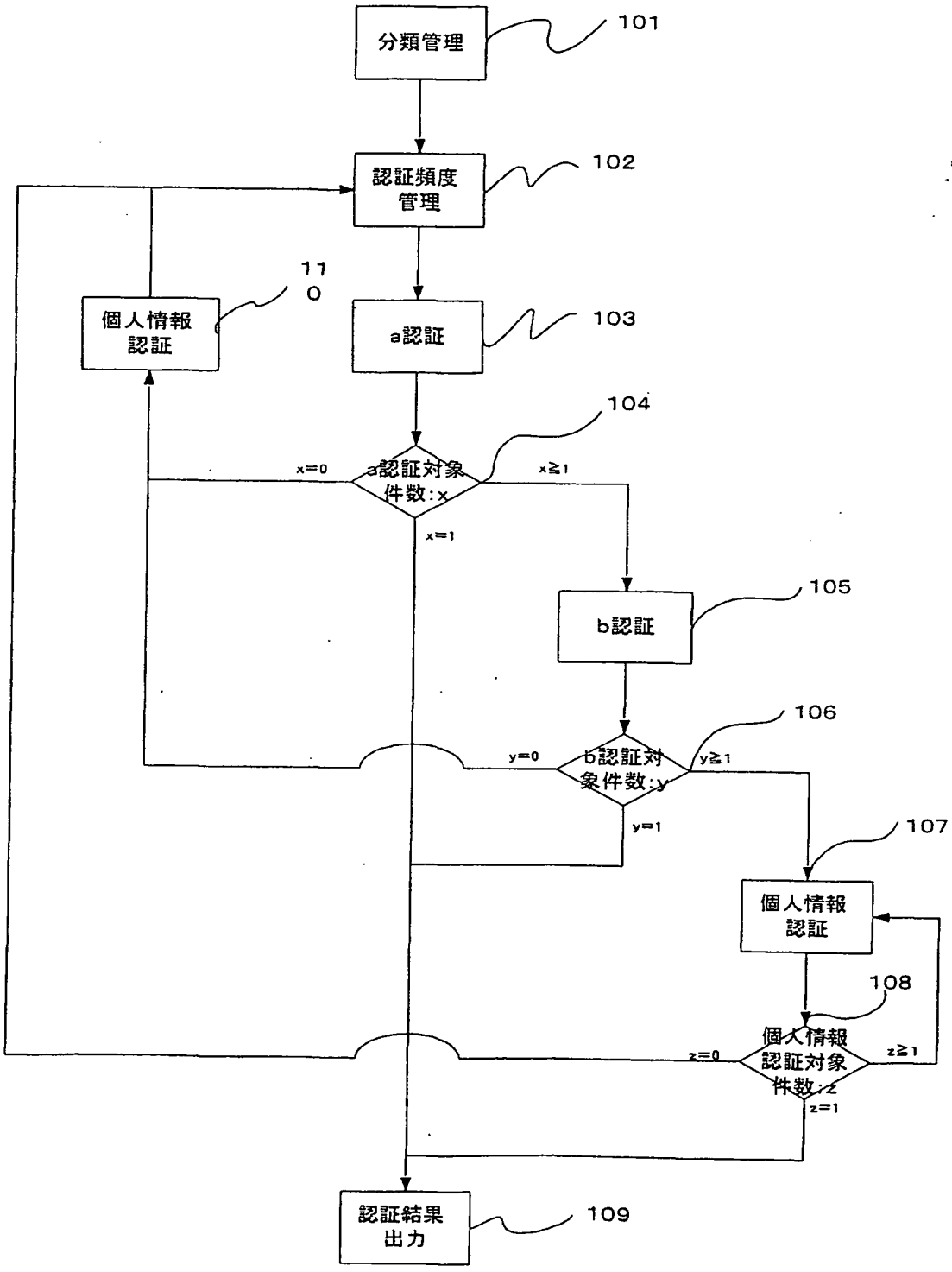

ステップ３０
ステップ３１
ステップ３９
ステップ３１
ステップ３２
対象有り？
ＮＯ
ＹＥＳ
ステップ３３
ステップ３４
対象有り？
ＮＯ
ＹＥＳ
ステップ３５
対象データは１？
ＹＥＳ
ＮＯ
ステップ３６
ステップ３８
いくつ？
２以上
０
１
ステップ３７

図 6


分類管理
101
認証頻度管理
102
個人情報認証
110
a認証
103
a認証対象件数:x
104
x=0
x≧1
x=1
b認証
105
b認証対象件数:y
106
y=0
y≧1
y=1
個人情報認証
107
個人情報認証対象件数:z
108
z=0
z≧1
z=1
認証結果出力
109

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/06418

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, 19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI biometrics*authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 3-288954 A (Hitachi, Ltd.), 19 December, 1991 (19.12.91), page 2, lower right column, line 5 to page 3, upper right column, line 10 (Family: none)	1-33
Y	JP 2-111132 A (Secom Co., Ltd.), 24 April, 1990 (24.04.90), page 2, lower left column, line 14 to page 3, upper left column, line 19 (Family: none)	1-33
A	WO 95/26013 A1 (Minnesota Mining and Manufacturing Company), 28 September, 1995 (28.09.95), Full text & US 5719950 A & JP 9-510636 A	1-33
A	JP 9-204401 A (NEC Corporation), 05 August, 1997 (05.08.97), page 1, column 1, line 2 to page 3, column 3, line 27 (Family: none)	1-33

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 December, 2000 (22.12.00)	16 January, 2001 (16.01.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP00／06418

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　　G06F15／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　　G06F15／00, 19／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2000年
日本国実用新案登録公報	1996－2000年
日本国登録実用新案公報	1994－2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI　biometrics＊authentication

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 3－288954, A（株式会社日立製作所）, 19. 12月. 1991（19. 12. 91）, 第2頁, 右下欄, 第5行－第3頁, 右上欄, 第10行（ファミリーなし）	1－33
Y	JP, 2－111132, A（セコム株式会社）, 24. 4月. 1990（24. 04. 90）, 第2頁, 左下欄, 第14行－第3頁, 左上欄, 第19行（ファミリーなし）	1－33
A	WO, 95／26013, A1（MINNESOTA MINING AND MANUFACTURING COMPANY）, 28. 9月. 1995（28. 09. 95）, 全文&US, 5719950, A&JP, 9－510636, A	1－33
A	JP, 9－204401, A（日本電気株式会社）, 5. 8月. 1	1－33

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　22. 12. 00	国際調査報告の発送日　16.01.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5M　8837 石井　茂和 電話番号　03－3581－1101　内線　6438

様式PCT／ISA／210（第2ページ）（1998年7月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	９９７（０５．０８．９７），第１頁，第１欄，第２行－第３頁，第３欄，第２７行（ファミリーなし）	